Ye et al. EURASIP Journal on Wireless Communications and Networking (2016) 2016:192
DOI 10.1186/s13638-016-0692-3

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A security fault-tolerant routing for multi-layer non-uniform clustered WSNs

Zhengwang Ye[1,3*], Tao Wen[1,2], Zhenyu Liu[1,2], Xiaoying Song[1] and Chongguo Fu[1,2]

Abstract

Wireless sensor networks have been studied extensively for their broad range of applications, especially in an environment with no infrastructure. And the nodes failures, link errors, and malicious node attacks are likely to occur quite frequently in wireless sensor networks. It affects the stability and reliability of data transmission. In this paper, we present a security fault-tolerant routing for multi-layer non-uniform clustered wireless sensor networks to improve the security reliability of network operation and data transmission. First, we establish the multi-layer non-uniform clustered network topology, which can effectively avoid the intercluster load imbalance; clustering can effectively reduce the network energy consumption and improve the network reliability. In the cluster head selection process, the trust model and the fuzzy logic are utilized to evaluate the qualification of sensors to become a cluster head. The routing algorithm uses the priority level and the trust value to select the security cluster head as the next hop and builds a route path between the different layers through the cluster head. Secondly, according to the multi-layer of the network topology structure, we present a fault-tolerant algorithm based on rollback strategy. Theoretical analysis and simulations show that the algorithm has the high packet receiving rate by BS and balanced energy consumption. It has good performance in fault tolerance and stability of data transmission, it avoids the hot issue in energy consumption and achieves the network load balance, and it prolongs the entire network life time.

Keywords: Wireless sensor networks, Routing algorithm, Fuzzy logic, Clustering, Security and reliable

1 Introduction

With the recent development in wireless sensor networks (WSNs) and multi-functional sensors with digital processing, power supply, and communication capabilities, WSNs are being largely deployed in physical environments for fine-grain monitoring in different types of applications [1]. But in addition to the power constraint, WSNs are prone to failure as they are deployed in a very harsh environment. Failures of nodes or links often occurred which lead to data loss or retransmission that seriously affects the data receiving rate, accuracy rate, and the average transmission delay. It lowers the transmission stability and reliability and weakens the reservation function, which brings great challenges to the existing network technologies [2].

The security and reliability of data transmission are important to evaluate the performance of WSNs. The establishment of the stable network topology realizes the effective and reliable data transmission, which needs to consider the balance of energy consumption, low transmission delay, and so forth [3]. So, it is necessary to build the topology of WSNs with stable data transmission, high energy consumption, and low transmission delay. Clustering has been proven to be one of the most effective techniques for reducing energy consumption of the WSNs in [4–9]. And the stable transmission of the network can be realized according to the fault-tolerant routing mechanism when the node has a failure or loss of link. The reasonable fault-tolerant can deal with faults in time when the node or link failure occurs, which can improve the reliability and stability of WSNs. So power efficiency and fault tolerance are essential properties to have for WSNs in order to keep the network functioning properly in case of energy depletion, hardware failures, communication link errors, or adverse environmental conditions, events that are likely to occur quite

* Correspondence: zhengwang119@126.com
[1]School of Computer Science and Engineering, Northeastern University, Shenyang, China
[3]Department of Network Information Center, Tonghua Normal University, Tong Hua, Jilin Province, China
Full list of author information is available at the end of the article

frequently in WSNs [10, 11]. In many fault-tolerant works such as [12–18], they have not considered the security of the network and the insider attacks of a malicious node. In pursuit of securing WSNs, the trust- and reputation-based schemes have proved to be more resilient against the insider attacks or node misbehavior attacks. So, we establish a security fault-tolerant routing based on the trust mechanism for multi-layer non-uniform clustered WSNs.

According to the limited characteristics of WSNs, considering the network lifetime, load distribution, malicious attacks, and fault-tolerance mechanism, a security fault-tolerant routing for multi-layer non-uniform clustered WSNs is proposed. First, we establish the multi-layer and non-uniform clustered topology. The network is divided into multi-layers according to the Euclidean distance between nodes and the sink node. The nodes of each layer are divided into clusters. The number of the cluster heads of each layer is determined by the number of nodes of the layer and the distance from the layer to the sink. The farther the distance from the sink to the layer is, the less number of the cluster heads is. Instead, the closer the distance from the sink to the layer is, the more number of the cluster heads is. The aim is to reduce the data forwarding task of the sensor nodes near the sink and balance the network load. In the cluster head selection process, the trust model and the fuzzy logic are utilized to evaluate the qualification of sensor nodes to become a cluster head. The trust value uses the packet forwarding ratio to evaluate. The trust model can detect malicious node to make sure the network is secure. The calculation of the priority of the node by layer uses three fuzzy parameters. They are the nodes' relative energy, relative density, and relative centrality. The cluster head selection takes into account the energy and position information of the nodes, so that the cluster heads have enough energy to work. In addition, due to the dynamic of WSNs, the cluster head selection algorithm should establish the cluster maintenance algorithm to make sure of the rationality of the cluster head selection. Secondly, according to the network topology structure, we present a security fault-tolerant routing algorithm. The routing is established based on the trust scheme and rollback strategy, which is different from the previous researches on the reliability and fault tolerance, the proposed method establishes an optimal routing path between adjacent layers and selects the highest priority and the trust cluster head as the next hop. When a cluster head is at fault or losses links, fault-tolerant routing algorithm is triggered. It uses a fallback strategy to re-select a new cluster head as the next hop of the routing path, and the routing maintenance retransmission mechanism does not establish a multi-hop path redundancy retransmission from the source node to the sink but through the back-off algorithm to back the upper layer of the fault cluster head and then re-choose a cluster head to establish the transmission path, this transmission mechanism reduce energy and delay of the network. The simulations show that the algorithm has the good performances in fault tolerance and security, and it avoids the hot issue in energy consumption and achieves the network load balance and prolongs the entire network life time.

The rest of the paper is organized as follows. In Section 2, the related works are introduced. In Section 3, the assumptions and network model are introduced. In Section 4, a multi-layer non-uniform clustering network topology is presented. In Section 5, based on the network topology, the security fault-tolerant routing is depicted, including its design idea and practical implementation approach. In Section 6, the simulations and the performance of the security fault-tolerant routing for multi-layer non-uniform clustered network are evaluated. Finally, conclusions are made in Section 7.

2 Related works

In recent years, a number of routing algorithms have been developed for clustered WSNs. Low-energy adaptive cluster hierarchy (LEACH) [4] is a popular clustering routing algorithm. The energy load of the network is distributed equally among each sensor node, so as to reduce the network energy consumption and prolong the entire network life time. But the cluster heads transmit directly data to the sink, the network may not scale for a larger sensor network, and the cluster heads communication power may not be enough to reach the sink. Recently in [5], the authors enhance the performance of the LEACH by balancing the energy consumption inside the clusters during the operation. Zhang and Chai [6] propose an unequal scale clustering algorithm considering node location constraint and node energy. The algorithm dynamically adjusts the cluster radius, real-time and effective process congestion, and cluster head fault to reduce the huge energy consumption of re-clustering process. In [7], the authors design a multi-hop routing and unequal clustering algorithm using residual energies of all the sensor nodes and distance between sensor nodes to the sink to extend the network lifetime. However, for a sensor node in this algorithm, it is very difficult to know the global information of all the other sensor nodes for a large scale networks. Bagci and Yazici [8] present an energy-aware unequal clustering algorithm with fuzzy. The algorithm adjacent to the region of the sink node is divided into many smaller clusters so that the load is more balanced. But the algorithm only considers the cluster node connectivity as a backup cluster head election basis, not considers the key influencing factor of residual energy. In [9], cluster head election

mechanism using fuzzy logic (CHEF) is proposed, which is a localized cluster head election mechanism. CHEF uses energy and local distance as fuzzy variables in the fuzzy if-then rules. Simulation results show that the cluster heads in CHEF are more evenly distributed over the network and then CHEF further prolongs the network lifetime. But CHEF does not construct multi-hop routes in cluster heads.

Moreover, there are some clustering routing algorithms which consider the fault-tolerant issues. They contain multi-path transmission routing [12], network coding [13], packets retransmission, and so forth. The direct diffusion (DD) [14] routing protocol is one of the most popular among them. In DD, if one of the paths is broken due to intermediate node failure, then another path is chosen to transmit the data. In [15], the authors propose a distributed energy efficient routing algorithm for WSNs that takes care of the fault tolerance of the gateways. It addresses the energy-efficient and fault-tolerant routing issues together. It avoids re-clustering but still can handle data routing in case of failure of some gateways. And it only considers permanent failure of the cluster head. In [16], the authors design a cluster-based routing protocol that groups sensor nodes to efficiently relay the sensed data to the sink by uniformly distributing energy dissipation among nodes and reducing latency for high-network data traffic. It is the representative of the fault tolerance in multi-player joint optimization and shows better performance. Li et al. [17] present a fault-tolerant routing algorithm based on the non-uniform hierarchical clustering inspired by the characteristics of vascular network. It applies the improved particles warm optimization to the non-uniform hierarchical clustering, and multi-paths are established between the neighbor hierarchical nodes based on the best-worst ant system. It has good performance in fault tolerance and stability of data transmission. In [18], the authors consider load balance and residual energy of two optimization objectives, present a cluster head selection mechanism based on an adaptively discrete particle swarm optimization, and give the fault-tolerance algorithm to ensure the cluster head two-connectivity. The algorithm can effectively guarantee the equilibrium of energy consumption, but the algorithm is computation-intensive. From the above discussion, the literatures do not consider the effect of the malicious attacks on security issues. Recently, mobile crowd sensing-based methods are studied based on social media data [19–21].

In the field of network security, the traditional security mechanisms such as cryptography and authentication are not mostly suitable for processing capability-constrained and energy-limited WSNs due to the complexity and huge computing memory [22]. In [23], the authors propose a secure routing in WSNs by splitting the network in layers. The security mechanism is established based on the encryption of message with a key-chain. As the message is routed, it is encrypted and decrypted as it makes to ensure the security of the message. But, this security mechanism cannot defend the insider or malicious attacks. As discussed in [24], the traditional security mechanisms are widely used to deal with external attacks but cannot solve insider or node misbehavior attacks effectively which are caused by the captured nodes. And the trust- and reputation-based schemes have proved to be more resilient against insider or node misbehavior attacks. To the best of our knowledge, lots of state-of-the-art secure routing have been proposed in this field [25, 26].

3 System model

The security fault-tolerant routing is developed with the following underlying assumption and models.

3.1 Assumption and network model

In this paper, we consider a scenario in which all the sensor nodes are randomly deployed in a two-dimensional space. Nodes are neither added nor removed from the network after deployment. It assumes that sensor nodes have the same capability of computing, communicating, and storing initial energy level and communication range. Their communication ability is limited by specific wireless techniques. And the interference range d_0 is equal to the transmission range. Only when two nodes take into each other's communication range could start communication. Each node keeps a list of neighbor nodes which stores their unique ID, exact location, communication information, neighbor list, the priority, and trust relationship. It assumes that all communication links are bidirectional and the communication channel is secure. All the sensor nodes can be the cluster head and common node, each node has enough computing power to complete the algorithm.

3.2 The energy model

According to the communication distance between the transmitting node and the receiving node, we use the same radio model for energy consumption as discussed in [4] in both the free space and multi-path fading channels. The energy required E_t by the radio to transmit a k-bit message over a distance d is given by:

$$E_t = \begin{cases} \left(E_{\text{elec}} + d^2 \times E_{\text{amp1}}\right) \times k & d < d_0 \\ \left(E_{\text{elec}} + d^4 \times E_{\text{amp2}}\right) \times k & d \geq d_0 \end{cases} \quad (1)$$

Free-space model is used when the distance is less than a threshold value d_0; otherwise, multi-path model is used. The E_{elec} is the energy required by the electronics circuit and E_{amp1} and E_{amp2} are the energy required by

amplifier in free space and multi-path, respectively. The energy required E_r by the radio to receive a k-bit message is given by:

$$E_r = k \times E_{elec} \tag{2}$$

4 Establish the multi-layer non-uniform clustered network topology

From the above discussion, the security, fault-tolerant, the energy, load balance, and the entire network life time are considered. We propose a multi-layer non-uniform clustered network topology to effectively manage the network energy consumption and improve the entire network performance.

4.1 The multi-layer model

According to the distance between the nodes and the sink, the network nodes are divided into different layers, the interference range is d_0, and assume the network is divided into L layer. Let dist (s, i) be the distance between the node i and the sink. The node i belong to the layer L_i is expressed as:

$$L_i = \left[2 * \frac{\text{dist}(s, i)}{d_0}\right] \tag{3}$$

And $L = \max(L_i)$, $i = 1, 2....$

As we know, the ones closer to the sink have higher pressure. Different quantities and densities of the clusters are presented in different layers. Hence, the number of the cluster head in different layer is determined by the number of nodes of the layer and the distance between the layer and the sink. The number of the cluster head *CH(i)* of *i*th layer is inversely proportional to the number of layers L_i and is proportional to the number of nodes N_i in the L_i layer. The number cluster heads CH*(i)* of the *i*th layer is calculated as follows:

$$\text{CH}(i) = \left[k_0 * \frac{N_i}{L_i}\right] \tag{4}$$

where k_0 is an adjustable parameter. The multi-layer model of the network is shown in Fig. 1.

4.2 The trust model

The packet forwarding ration is a measure of the number of correctly forwarding packets to the number of packets supposed to be forwarded. We use the packet forwarding ration as the trust value of the node. It is expressed as [27]:

$$T_{i,j}(t) = \frac{F_{i,j}(t)}{R_{i,j}(t)} \tag{5}$$

Where, $T_{i,j}(t)$ is the trust value node i to node j at time t, $F_{i,j}(t)$ represents the number of packets forwarded correctly by node j at time t, and $R_{i,j}(t)$ represents and signifies the number of packets successfully received by node j from node i at time t.

It is known that the calculation of the packet forwarding ration comes from different neighbor nodes. So, the trust value can be expressed as:

$$\text{TA}_j(t) = \frac{\sum_{i=1}^{m} T_{i,j}(t)}{m} \tag{6}$$

where m represents the neighbor number of node j. $\text{TA}_j(t)$ represents the trust value of node j.

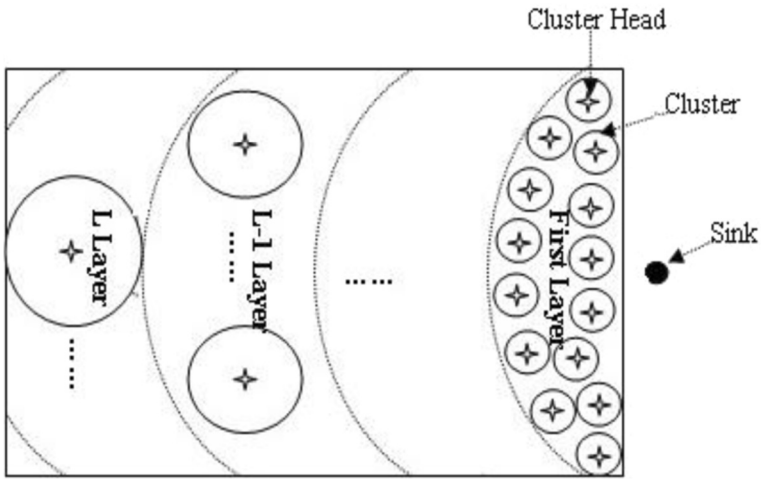

Fig. 1 The multi-layer model of the network

4.3 The nodes' priority

Fuzzy logic is a powerful tool that can make a decision even if there is insufficient data, while sufficient data is needed for making a decision in classic control. In [9], fuzzy logic is used for routing and improving the network lifetime. We also use fuzzy logic to select cluster heads. After a sensor network is layered, according to the fuzzy variable and fuzzy rules, the priority of node is calculated and the priority is an important factor for the cluster head selection. For each layer, the cluster head can only communicate with the cluster head in different layers and cannot communicate with the same layer cluster head. That makes sure the data transmission is isotropic.

4.3.1 The fuzzy input and output variables

The cluster head in the network is very important. There are some factors that can affect the cluster head selection mechanism. As discussed in [9], three fuzzy variables (energy, concentration, and centrality) are used for fuzzy if-then rule. In [28], the authors propose a two-level fuzzy logic to evaluate the qualification of sensors to become a cluster head. Three fuzzy parameters are centrality, proximity to the sink, and distance between cluster heads. In [29], the fuzzy logic-based clustering scheme parameters used to select cluster head are residual energy, base station distance, concentration, and local distance. In this paper, the cluster head selection is evaluated according to node physical characteristics of residual energy, the distance among cluster heads, and its neighbor nodes density. Longer network lifetime is achieved when the overall cluster heads' energy consumption is less, which is directly related to the nodes proximity to cluster heads. And the centrality metric makes a cluster more load balanced when adjacent nodes send their data to a cluster head. To balance the energy consumption, there must be sufficient distance among cluster heads. So, we use the relative energy, the relative density, and the relative centrality of a node as the fuzzy input variables.

(1) The node relative energy

The relative energy $R_{\mathrm{E}}(i)$ of node i is the ratio of node i's residual energy E_i to the maximum residual energy $E_{\max}$ in a cluster. The value expresses the rest remaining energy of node i inside the cluster. It is expressed as:

$$R_{\mathrm{E}}(i) = \frac{E_i}{E_{\max}} \tag{7}$$

(2) The node relative density

The node density represents the intensity of nodes density, which represented by the number of neighbor nodes D_i in the communication range of d_0. The node density is higher, and the energy consumption of the neighbor nodes is lower. The relative density $R_{\mathrm{D}}(i)$ of node i is the ratio of node i's density D_i to the maximum density $D_{\max}$ in a cluster. It is expressed as:

$$R_{\mathrm{D}}(i) = \frac{D_i}{D_{\max}} \tag{8}$$

(3) The node relative centrality

The node centrality represents the closeness of nodes and neighbors. The formula is as follows:

$$C_i = \sqrt{\left(x_i - \frac{1}{n}\sum_{j=i}^{n} x_j\right)^2 + \left(y_i - \frac{1}{n}\sum_{j=i}^{n} y_j\right)^2} \tag{9}$$

where C_i is the node ith centrality, x_i represents the horizontal coordinates of node i, and y_i represents the longitudinal coordinates of node i. n represents the number of the neighbors.

It is known that the closer the cluster head to the neighbor nodes, the less the energy consumption is. So, we select the relative centrality as one of the fuzzy variables. The relative density $R_C(i)$ of node i is the ratio of the minimum centrality $C_{\min}$ to node i's density C_i in a cluster. It is expressed as:

$$R_C(i) = \frac{C_{\min}}{C_i} \tag{10}$$

(4) The nodes priority

From the above, we know the relative energy, the relative density, and the relative centrality of a node as the fuzzy input variables. Based on the input variables, we can get the nodes' priority as the output variables. And the node priority determines whether the node can become the cluster heads. Then, we give the corresponding fuzzy sets which are mapped to the variables and also give the membership function of each fuzzy set. The acquisition of the fuzzy sets is based on the objective existence of the problem, people's practical experience, and valuable significance. Triangle and trapezoidal membership functions are used because they are suitable for real-time systems [30]. The relative energy membership function, the relative density membership function, and the relative centrality membership function are shown in Fig. 2a–c, respectively. The out parameter of the nodes priority is very low, low, rather low, medium, rather high, high, very high. The relationship between the nodes priority membership function and the feature set is shown in Fig. 2d.

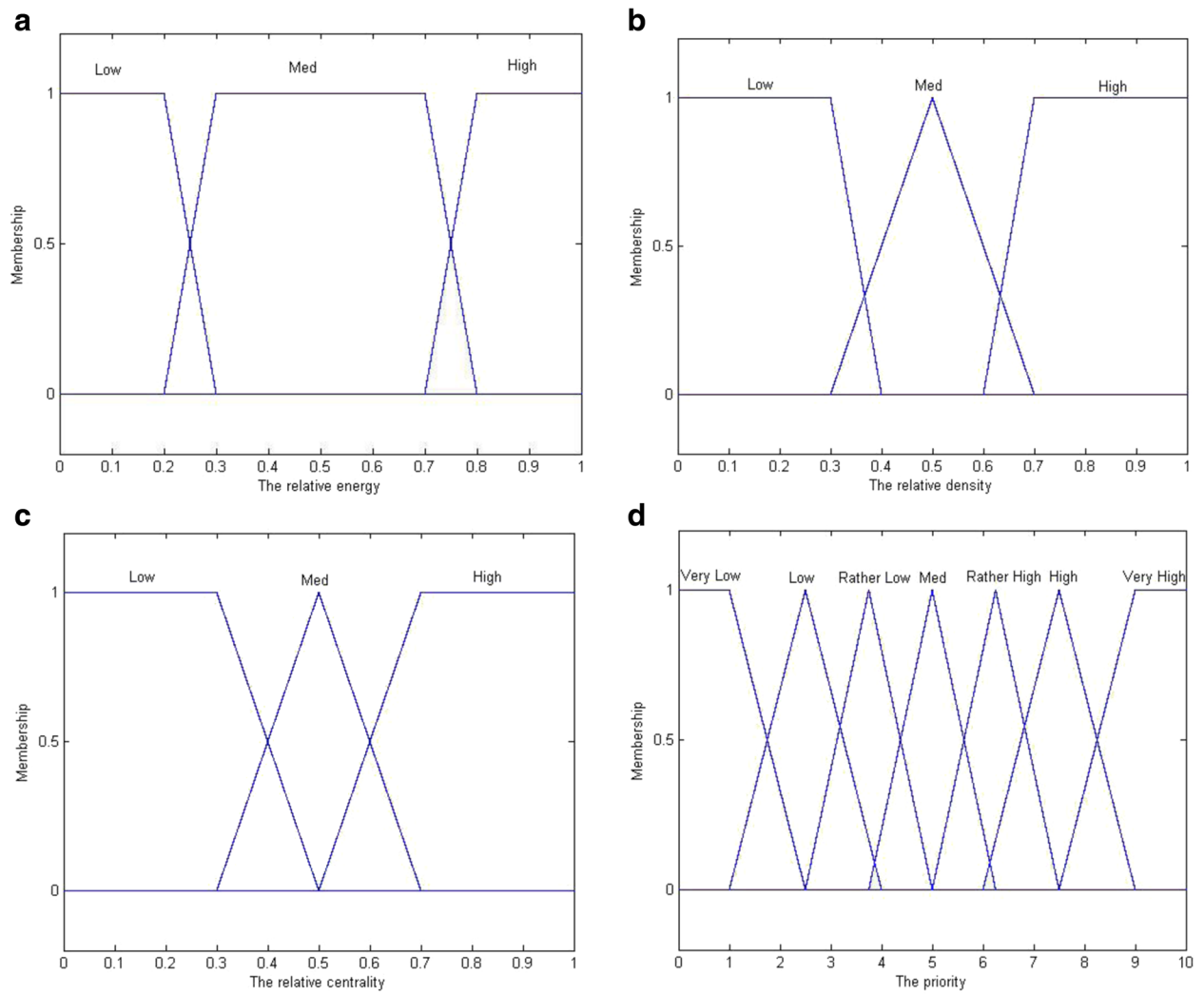

Fig. 2 Membership functions of the input and output variables. **a** Membership functions of the relative energy. **b** Membership functions of the relative density. **c** Membership functions of the relative centrality. **d** Membership functions of the node priority

4.3.2 The fuzzy rules

In this paper, the relative energy, the relative density, and the relative centrality are defined as the inputs to the fuzzy system and the priority of a node is the output. So, if the relative energy, relative density, and the relative centrality are high, the priority of the node is very high, too. The fuzzy if-then rules are shown in Table 1.

4.3.3 The nodes priority

According to the output of the fuzzy rules, we can get the actual value of the priority value. In [9], the authors use the center-of-area as a defuzzification method. In this paper, we use the center-of-gravity for defuzzification because they are more similar. But the center-of-gravity is more accurate. The formula is as follows:

$$\mathrm{pri} = \frac{\int x\mu_{\mathrm{pri}}(x)dx}{\int \mu_{\mathrm{pri}}(x)dx} \tag{11}$$

where pri is the node priority, $\mu_{\mathrm{pri}}(x)$ is the fuzzy set membership function for the node priority, and x is the node priority value. So, we can get the priority of a node. Next, the selection algorithm of cluster head is introduced in detail.

4.4 The cluster head selection

The cluster head selection mechanism considers the trust value and the node priority together. First, we use Eq. (6) to get the trust value of a node. If $\mathrm{TA}_i < 0.5$, the node is considered as a malicious node or an unreliable node and marked in WSNs, and then according to the

Table 1 Fuzzy if-then rule

Rule ID	The relative energy	The relative density	The relative centrality	Node priority
1	Low	Low	Low	Very low
2	Low	Low	Medium	Very low
3	Low	Low	High	Very low
4	Low	Medium	Low	Very low
5	Low	Medium	Medium	Very low
6	Low	Medium	High	Very low
7	Low	High	Low	Very low
8	Low	High	Medium	Very low
9	Low	High	High	Very low
10	Medium	Low	Low	Rather low
11	Medium	Low	Medium	Rather low
12	Medium	Low	High	Medium
13	Medium	Medium	Low	Rather low
14	Medium	Medium	Medium	Medium
15	Medium	Medium	High	Rather high
16	Medium	High	Low	Rather low
17	Medium	High	Medium	Medium
18	Medium	High	High	Rather high
19	High	Low	Low	Rather low
20	High	Low	Medium	Medium
21	High	Low	High	Rather high
22	High	Medium	Low	Medium
23	High	Medium	Medium	Rather high
24	High	Medium	High	High
25	High	High	Low	Medium
26	High	High	Medium	High
27	High	High	High	Very high

high-ranking priority per layer, we select CH*(i)* records from the ranking as cluster head. And the other nodes which have not been selected as cluster heads join the nearest cluster head to form clusters.

4.5 The establishment of multi-layer non-uniform clustered topology

The multi-layer non-uniform clustered topology is established based on the above analysis. The detail steps of the multi-layer non-uniform clustered topology are as follows:

Step 1: Initialize the parameters, including the number of the nodes, and the initialize trust value. We calculate the network topology layers according to Eq. (3). We get the maximum number of network layer L based on the distance.
Step 2: Calculate the layer L_i of node i using the Eq. (3).
Step 3: Calculate the number of cluster heads CH(i) in the ith layer by Eq. (4). At first, we randomly select CH(i) nodes as cluster heads from the ith layer.
Step 4: Initialize clusters. According to the number of nodes per layer and the number of cluster heads CH(i), initialize the clusters by layers. And the other nodes which have not been selected as a cluster head join the nearest cluster head to form clusters.
Step 5: Update clusters after a few rounds. The trust value is calculated according to Eq. (5) and (6). The cluster head selection mechanism is trigged according to the trust value and the priority of nodes. We can get the sequence of cluster heads in each layer. We select CH(i) records from the sequence as a cluster head to form new clusters.
Step 6: Establish the routing path according to the sequence of cluster heads in each layer and complete data transmission. After Δ rounds, go to step 5 and update the clusters.

5 The security fault-tolerant routing

The multi-hop transmission routing is established according to the cluster heads among different layers. We evaluate the security of the cluster head according to the trust value. We use the priority level of each layer cluster head to select the optimal path, which reflects nodes' energy, density, and centrality. The routing path with priority factor maximum overall cluster heads as the highest trust value is selected to take part in packet forwarding. For example, if a node is a trusted one and it has the highest priority, its upstream node may add that cluster head in an active route. However, if a node is reliable but does not have the highest priority, its request packet is ignored during a route discovery process. Similarly, if a node has the highest priority but is not trusted, its request may also be ignored by its upstream node. In addition, the fault-tolerant is considered in the routing maintenance process. The fault-tolerant algorithm is started when the selected cluster heads failure or lost. The detail steps of the routing are as follows:

Step 1: Initialize the network. According to the number of nodes of each layer and the number of cluster heads, initialize the clusters.
Step 2: Update clusters. The cluster heads selection mechanism is trigged according to the trust value and the priority of nodes. We can get the sequence of cluster heads in each layer. We select CH(i) records from the sequence as a cluster head to form new clusters.
Step 3: Establish routing path. The multi-hop route path is established among different layer cluster heads. The routing path is from the source node to the cluster

head of the $L_{i\text{th}}$ layer with the highest priority, and then to the cluster head of the *(L-1)*th layer with the highest priority until the sink. And then transmit the data packet.
Step 4: If round = T or the cluster head residual energy is below half of the average residual energy within the cluster, then return to step 2. If an intermediate cluster head finds packet forwarding misbehavior caused by faulty or failure on active path, go to step 5.
Step 5: The fault-tolerance routing algorithm. When an intermediate cluster head is a failure or lost, fault-tolerant routing algorithm is trigged. The abnormal node rollbacks to the upper layer of a failure cluster head and re-chooses a new cluster head with the highest priority as the next hop to complete the task of transmission.

In the whole process, the network is dynamic, and we need to update the cluster heads by layer periodically. We define that the whole network update each T seconds. When the $L_{i\text{th}}$ layer in a cluster head residual energy is below half of the average residual energy within the cluster, the cluster heads re-select and re-create clusters in L_i, and to establish $L_i + 1$ layer to L_i layer and L_i layer to layer $L_i - 1$ data forwarding path.

Consider a network shown in Fig. 3 as an example, which assumes source node as the sender and the sink as the receiver. The multi-layer non-uniform clustering topology is established like as show in Fig. 3, which includes three layers with different numbers of cluster heads. The routing path is established among the cluster heads in different layers within their transmission power coverage. As shown in Fig. 3, there is only a path selected as the transmission path and the others are the backup transmission paths for the fault-tolerance. When an intermediate cluster head is a failure or lost, fault-tolerant routing rollbacks to the upper layer of failure cluster head re-choose a new cluster head with the highest priority as the next hop to complete the task of transmission and ensure the robustness and reliability of the network.

6 Simulations and analysis

Our experiments are performed using MATLAB to analyze the performances of our algorithm in this section. The concrete simulation scene is set to be 200 m × 200 m, with 200 randomly deployed sensor nodes. Some parameters vary with the scenes, and the purposes of experiment will be explained in detail. The initial values of the other simulation parameters are shown in Table 2.

6.1 Multi-layer non-uniform topology of the network

Based on the parameters in Table 2, Fig. 4 shows that 200 sensor nodes are randomly deployed in the area [200, 200]. These nodes are not divided by layers, and all nodes have the same property. The sink node is deployed at (250, 100). According to the topology's structure of WSNs, we can get the number of layers of the WSNs which is $L = 6$. Each node is layered according to the distance from the sink. The nodes in Fig. 5 are divided into different layers based on Fig. 4. As show in Fig. 5, the nodes of each layer have different symbol markers.

6.2 Multi-layer non-uniform clustering

According to the multi-layer model, we can get the multi-layer distribution of the network nodes as show in Fig. 5. And different clusters are adopted in different layers. Using Eq. (4), we get the number of the cluster heads of each layer. We used the cluster heads selection

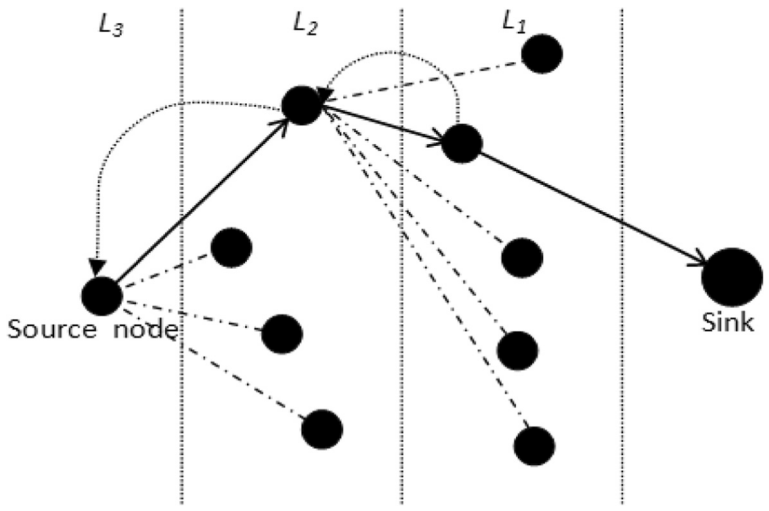

Fig. 3 The routing establishment and maintenance

Table 2 Simulation parameters

Parameters	Value
Initial energy	0.5 J
Initial trust value	0.5
d_0	87 m
Packet length	2000 bit
E_{elec}	50 nJ/bit
E_{amp1}	10 pJ/bit/m^2
E_{amp2}	0.0013 pJ/bit/m^4
T	Δ

algorithm to select cluster heads by layers. Finally, it forms the cluster heads distribution as shown in Fig. 6. Different layers of the cluster heads express different symbols. Figure 6 shows that the cluster heads are distributed non-uniformly. It forms the distribution with larger amount of the cluster heads in the layer where it is near to the sink. And so does the opposition in the layer where it has fewer cluster heads in the layer where it is far from the sink.

6.3 Multi-layer non-uniform routing establishment and maintenance

After the multi-layer division and non-uniform distribution of the static clustering, the cluster heads selection algorithm is executed based on the trust value and the priority. According to the fuzzy logic rules in Table 1, the priority of each node is obtained by layer. The cluster heads are updated periodically with the trust value and the priority of node. In the simulation, the process of an intercepting routing path is shown in Fig. 7. From Fig. 7, the multi-hop routing path is established according to the cluster heads in different layers which has the highest priority. But when a cluster head or a link failure

Fig. 4 Random distribution of sensor nodes

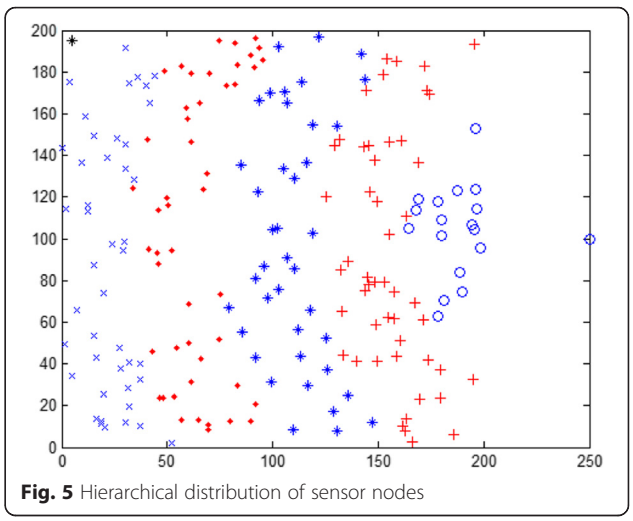

Fig. 5 Hierarchical distribution of sensor nodes

or lost in the multi-hop routing path, the maintenance of the routing is trigged. As shown in Fig. 7, in the second layer, the cluster heads failed, the route maintenance strategy uses the fault-tolerance mechanism through rollback to the failure cluster head upper layer and re-chooses the next hop to complete the task of transmission and ensure the robustness and reliability of the network.

6.4 Analysis of energy consumption and network lifetime

The multi-layer non-uniform clustering topology is used for WSNs in this paper. As mentioned before, it can reduce the data forwarding task of sensor nodes near the sink and balance the network load consumptions. Moreover, the cluster heads transfer the fusion data to the Sink layer by layer, establish a multi-hop route, and reduce the energy consumption between the sink and the cluster heads. Our algorithm, LEACH in [4], and CHEF in [9] residual energy comparison is shown in Fig. 8. As show in Fig. 8, the residual energy of our algorithm is

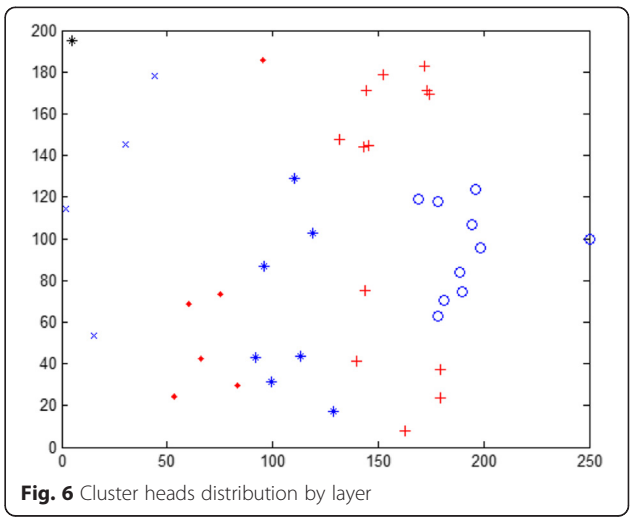

Fig. 6 Cluster heads distribution by layer

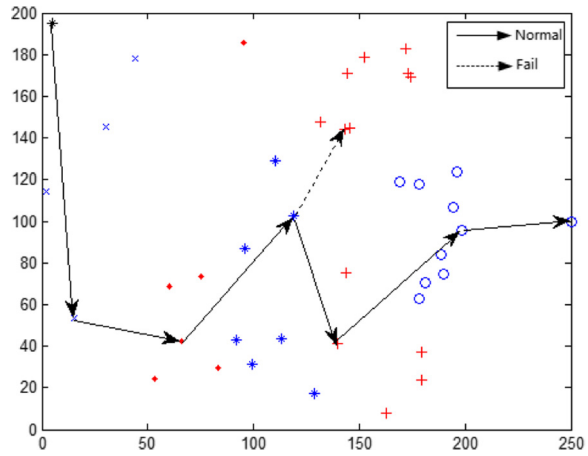

Fig. 7 Transmission route path

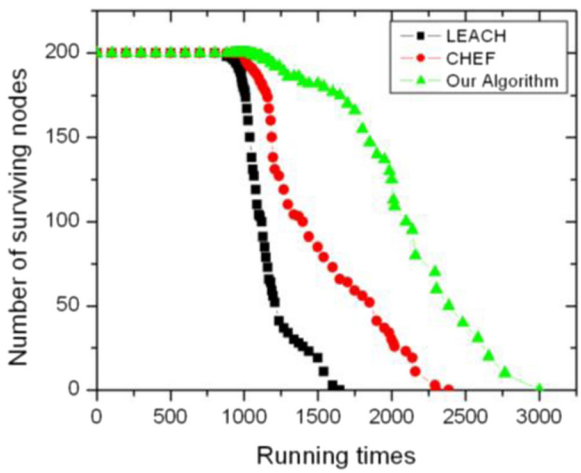

Fig. 9 The comparison of the network lifetime

significantly higher than that of LEACH and CHEF, which shows that the residual energy of our algorithm is larger, so the running consumes less energy and can effectively prolong the network lifetime. Our algorithm, LEACH and CHEF network lifetime comparison is shown in Fig. 9. From Fig. 9, we can get our algorithm network lifetime much longer than the LEACH. And in our algorithm, the first dead node appear much later than the LEACH and CHEF, which means the WSNs of our algorithm can work over a longer period of time without the nodes failure and enhance the performance and efficiency of the whole network effectively.

6.5 Performance analysis of the security and the fault tolerance

In our algorithm, we use the trust model to evaluate the security of the cluster head. And also the fault-tolerant routing mechanism is established to complete the maintenance of the routing. As discussed above, the multi-hop routing path is established between the cluster heads in neighbor layers within their transmission power coverage, the trust value and the priority of cluster head is the basis of the selection of data transmission path, but only the security cluster head with the highest priority is to be selected as the actual data transmitting path. First, we assume that the fault nodes in the network are supposed to be the ones in which the energy consumption reaches the initial threshold value and not have any malicious node. We make a comparison with the present algorithm DD in [14], CPEQ in [17], and our proposed algorithm in the receiving rate shown in Fig. 10. As show in Fig. 10, with the increasing number of operation times, the fault nodes' number also increases. The proposed algorithm has a better performance in the packet receiving rate and reflects the good stability in data transmission than the DD and CPEQ.

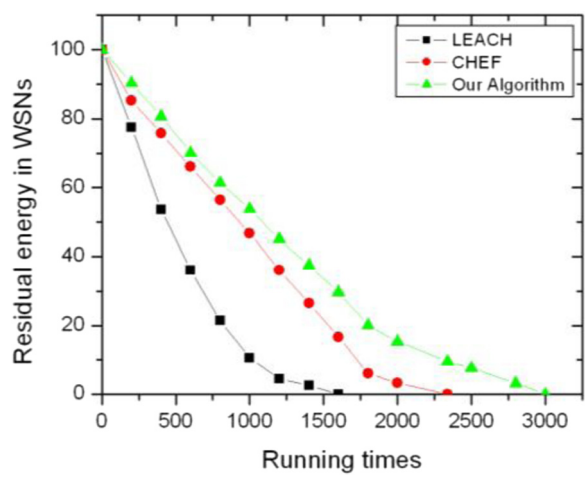

Fig. 8 The comparison of the residual energy

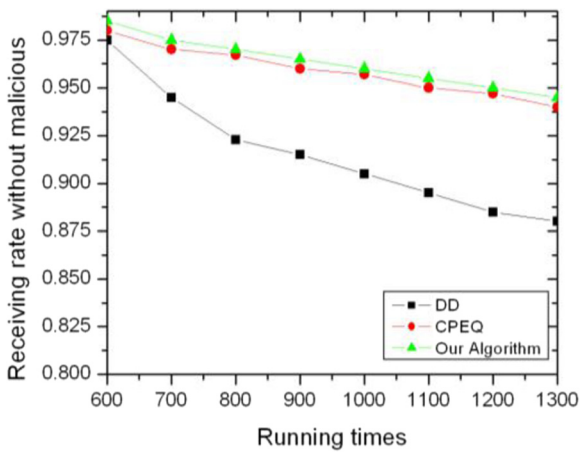

Fig. 10 Comparison of packet receiving rate without malicious

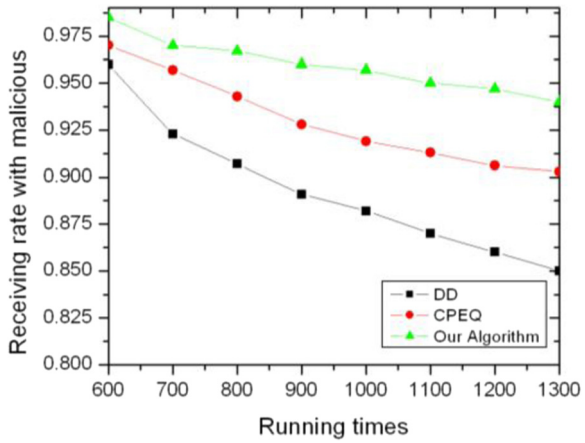

Fig. 11 Comparison of packet receiving rate with malicious

Second, we assume that the fault nodes in network are supposed to be the ones in which the energy consumption reaches the initial threshold value and have 10 % malicious nodes. We make a comparison with DD and CPEQ again, and the receiving rate is shown in Fig. 11. As show in Fig. 11, the receiving rate of the packets is compared to Fig. 10 rapid descent. Our proposed algorithm change a little, which shows the proposed algorithm effective identification of the impact of malicious nodes on data transmission. From the above discussion, we know that the proposed algorithm has a high packet receiving rate by BS. It not only has the performance of the fault-tolerance against sensor node failure or lost but also has the security against malicious nodes, that makes sure the network data transmission is more secure and stable.

7 Conclusions

In this paper, we present a multi-layer non-uniform clustering fault-tolerant routing algorithm. We establish the multi-layer non-uniform clustered network topology, which can effectively avoid the intercluster load imbalance, reduce the network energy consumption, and improve the network reliability. In the cluster head selection process, the trust model and the fuzzy logic are utilized to evaluate the qualification of sensor nodes to become a cluster head and form the cluster. The routing algorithm uses the trust value and the priority of nodes to select the cluster heads and build clusters. The route of path is established between different layers through the cluster heads. To improve the security and the fault-tolerant of the network, we present a fault-tolerant routing algorithm based on rollback strategy. Theoretical analysis and simulations show that the proposed algorithm has high packet receiving rate by BS and balanced energy consumption. It has good performance in fault tolerance and stability of data transmission, and it avoids the hot issue in energy consumption and achieves the network load balance, and it also prolongs the entire network life time.

Acknowledgments

This research is supported by the National Nature Science Foundation of China (61170169, 61170168)

Authors' information

Zhengwang Ye, the corresponding author, received BS degree in Computer Science from China West Normal University, China, in 2008. He is currently a Ph.D. candidate at the Department of Computer Science at Northeastern University, China. His current research interests are network security, trust management, and routing algorithm for wireless sensor networks.

Wen Tao is a PhD supervisor at Northeastern University, China. He received his Ph.D. degree from Northeastern University, China, in 1993. Since 2000, he has been the president of Dalian Neusoft Institute of Information, China. He has authored more than 60 refereed journals and conference papers. His research interests are network security, wireless sensor networks, and service-oriented computing.

Zhenyu Liu received BS degree in Computer Science from China Jilin University, China, in 2004. He is currently a Ph.D. candidate at the Department of Computer Science at Northeastern University, China. His current research interests are network security and routing algorithm.

Xiaoying Song received her B.Sc. and M.Sc. degrees in computer science from Shenyang University of Technology, China, in 2007 and 2010, respectively. She is currently a Ph.D. candidate at the Department of Computer Science at Northeastern University, China. Her current research interests are wireless sensor networks and clustering routing algorithm.

Chongguo Fu, the corresponding author, received the BS degree in computer science from Tsinghua University, China, in 2002. He is currently a Ph.D. candidate at the Department of Computer Science at Northeastern University, China. His current research interest is security properties of distributed data storage for wireless sensor networks.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]School of Computer Science and Engineering, Northeastern University, Shenyang, China. [2]Department of Computer Science and Technology, Neusoft Information Institute, Dalian, Liaoning, China. [3]Department of Network Information Center, Tonghua Normal University, Tong Hua, Jilin Province, China.

Received: 31 May 2016 Accepted: 9 August 2016
Published online: 23 August 2016

References

1. K Akkaya, M Younis, A survey of routing protocols in wireless sensor networks. Elsevier Ad Hoc Network **3**(3), 325–349 (2005)
2. L Paradis, Q Han, A survey of fault management in wireless sensor networks. J Network & Syst Manage **15**(2), 171–190 (2007)
3. Y Yang, C Zhong, Y Sun et al., Network coding based reliable disjoint and braided multipath routing for sensor networks. J Network & Comput Appl **33**(4), 422–432 (2010)
4. WB Heinzelman, AP Chandrakasan, H Balakrishnan, An application-specific protocol architecture for wireless micro sensor networks. IEEE Trans Wirel Commun **1**(4), 660–670 (2002)
5. A Salim, W Osamy, AM Khedr, IBLEACH: intra-balanced LEACH protocol for wireless sensor networks. Wirel Netw **20**(6), 1515–1525 (2014)
6. Q Zhang, Q-l Chai, Unequal scaled clustering routing for WSN based on redundancy of cluster headers. Comput Eng **37**(14), 28–30 (2011)
7. B Gong, L Li, S Wang et al., Multihop routing protocol with unequal clustering for wireless sensor networks [C]//2008 ISECS International Colloquium on Computing. Communication, Control, and Management, IEEE, 552–556 (2008)

8. H Bagci, A Yazici, An energy aware fuzzy approach to unequal clustering in wireless sensor networks. Appl Soft Comput **13**(4), 1741–1749 (2013)
9. JM Kim, SH Park, YJ Han, TM Chung, *CHEF: cluster head election mechanism using fuzzy logic in wireless sensor networks* (Proceedings of International Conference on Advanced Communication Technology, Dublin, 2008), pp. 654–659
10. H Liu, A Nayak, I Stojmenović, *Fault-tolerant algorithms/protocols in wireless sensor networks [M]//In Guide to Wireless Sensor Networks, Springer: London, UK,* 2009, pp. 261–291
11. H Alwan, A Agarwal, A survey on fault tolerant routing techniques in wireless sensor networks [C]//Proceedings of International Conference on Sensor Technologies and Applications, 2009 (Sensorcomm. IEEE, 2009), IEEE, pp. 366–371
12. N Sun, Y Cho, S Lee, Node classification based on functionality in energy-efficient and reliable wireless sensor networks. Int J Distributed Sensor Networks **2012**, 12 (2012)
13. A Gluhak, S Krco, M Nati et al., A survey on facilities for experimental internet of things research. IEEE Commun Mag **49**(11), 58–67 (2011)
14. C Intanagonwiwat, R Govindan, D Estrin, Directed diffusion: a scalable and robust communication paradigm for sensor networks [C]//Proceedings of International conference on mobile computing and networking, 2000, ACM, pp. 56–67
15. M Azharuddin, PK Jana, A distributed algorithm for energy efficient and fault tolerant routing in wireless sensor networks. Wirel Netw **21**(1), 251–267 (2014)
16. A Boukerche, RWN Pazzi, RB Araujo, Fault-tolerant wireless sensor network routing protocols for the supervision of context-aware physical environments. J Parallel & Distributed Computing **66**(4), 586–599 (2006)
17. H Li, P Gao, Q Xiong et al., A vascular-network-based nonuniform hierarchical fault-tolerant routing algorithm for wireless sensor networks [J]. Int J Distributed Sensor Networks **6**, 150–160 (2012)
18. J Su, W Guo, C Yu et al., Fault-tolerance clustering algorithm with load- balance aware in wireless sensor networks. Chin J Comput **37**(2), 446–456 (2014)
19. Z. Xu et al, *Crowdsourcing based social media data analysis of urban emergency events. Multimedia Tools and Applications*. doi: 10.1007/s11042-015-2731-1.
20. Z. Xu et al, *Crowdsourcing based description of urban emergency events using social media big data* (IEEE Transactions on Cloud Computing). doi:10.1109/TCC.2016.2517638.
21. Z Xu, H Zhang, V Sugumaran, KR Choo, L Mei, Y Zhu, Participatory sensing-based semantic and spatial analysis of urban emergency events using mobile social media. EURASIP J Wireless Comm and Networking **2016**, 44 (2016)
22. J Cordasco, S Wetzel, J Cordasco et al., Cryptographic versus trust-based methods for MANET routing security. Electronic Notes in Theoretical Computer Science **197**(2), 131–140 (2008)
23. K Bairaktaris, I Chatzigiannakis, V Liagkou et al., Adaptive probabilistic secure routing in mobile wireless sensor networks [C]//Proceedings of International Conference on Software, Telecommunications and Computer Networks (IEEE, 2008), IEEE, pp. 208–212
24. M Momani, S Challa, Survey of trust models in different network domains. Int J Ad Hoc Sensor & Ubiquitous Computing **1**(3), 1–19 (2010)
25. G Han, J Jiang, L Shu et al., Management and applications of trust in wireless sensor networks: a survey. J Comput Syst Sci **80**(3), 602–617 (2014)
26. F Ishmanov, AS Malik, SW Kim et al., Trust management system in wireless sensor networks: design considerations and research challenges. Trans Emerging Telecommunications Technologies **26**(2), 107–130 (2015)
27. A Ahmed, KA Bakar, MI Channa et al., A trust aware routing protocol for energy constrained wireless sensor network. Telecommun Syst **61**(1), 123–140 (2016)
28. NA Torghabeh, MRA Totonchi, MHY Moghaddam, *Cluster head selection using a two-level fuzzy logic in wireless sensor networks [C]* (Proceedings of International Conference on Computer Engineering and Technology, 2010), IEEE, pp. V2-357–V2-361
29. AK Mishra, R Kumar, J Singh, A novel cluster head selection scheme using fuzzy logic in wireless sensor networks [C]//Proceedings of International Conference on Green Computing and Internet of Things (IEEE, 2015), IEEE, pp. 203–208
30. R Feng, S Che, X Wang, A credible cluster-head election algorithm based on fuzzy logic in wireless sensor networks. J Computational Information Systems **8**(15), 6241–6248 (2012)